Electronic Recording Delivery System

Computer Security Auditor Approval Handbook

DRAFT

VERSION 1

California Department of Justice
CJIS Operations Support Bureau
Electronic Recording Delivery System Program

ELECTRONIC RECORDING DELIVER SYSTEM (ERDS)
COMPUTER SECURITY AUDITOR APPROVAL HANDBOOK
TABLE OF CONTENTS

SECTION 11 Escrow Requirements

SECTION 12 Security Audit Requirements

SECTION 13 Appendices

Terms and Conditions – Auditor
Geographical Locations
Social Security Number Privacy Statement
Fee Schedule – PENDING
Disqualifying Offenses
Statutory Authority, Chapter 621
Statutory Authority, Chapter 520
Regulations – PENDING
Baseline Requirements and Technology Standards
Forms:
ERDS 0002 - Application for Computer Security Auditor Approval
ERDS 0004 - Computer Security Auditor Significant Experience Requirements, Attachment A
ERDS 0006 – Request for Replacement of Certificate or Application Documents
ERDS 0010 - Application for Withdrawal

(Fingerprinting Requirements Document)
BCII 9004 – Request for Exemption from Mandatory Electronic Fingerprint Submission Requirement
BCII 8016 – Sample Request for Live Scan Service
FD 258 – Fingerprint Hard Card

SECTION 1
INTRODUCTION

The Electronic Recording Delivery Act of 2004 authorizes a County Recorder, upon approval by resolution of the board of supervisors and system certification by the Attorney General, to establish an Electronic Recording Delivery System (ERDS) for the delivery and recording of specified digitized or digital electronic records that are an instrument of real estate transactions, subject to specified conditions, including system certification, regulation, and oversight by the Attorney General. (Government Code section 27390-et seq).

Individuals requesting Approval as a Computer Security Auditor must contact the ERDS program and request the Computer Security Auditor Approval Package. ERDS staff will inform the applicant of the availability of the Computer Security Auditor Approval Package on the Attorney General's website, http://ag.ca.gov/ or will, at the request of the applicant, send the package via ground mail.

Within the Attorney General's office, the ERDS Program within the Department of Justice has been established and is responsible for implementing the requirements of the law.

ERDS Program contact information:

Department of Justice
Electronic Recording Delivery System Program
P.O. Box 160526
Sacramento, CA 95816-0526

Telephone:	(916) 227-8907
Fax:	(916) 227-0595
E-mail address:	erds@doj.ca.gov
Website:	http://caag.ca.gov/erds

The following procedures establish the requirements to be met by an applicant to become an Approved Computer Security Auditor.

Applicants requesting to become an ERDS Approved Computer Security Auditor must read Section C of ERDS 0002, Application for Computer Security Auditor Approval and certify, by signing under penalty of perjury, that they understand and agree to the Terms and Conditions-Computer Security Auditors established by the Attorney General.

SECTION 2
DEFINITIONS

For a detailed explanation of the Definitions used throughout the process of establishing an Electronic Recording Delivery System, refer to the Baseline Requirements and Technology Standards information found in Section 13 – Appendices.

SECTION 3
CONTENTS OF COMPUTER SECURITY AUDITOR APPROVAL PACKAGE

The Computer Security Auditor Approval Package will contain the following material:

1. ERDS 0002, Application for Computer Security Auditor Approval, and ERDS 0004, Computer Security Auditor Significant Experience Requirements, Attachment A
2. BCII 8016 - Request for Live Scan Service – Preprinted with the ERDS Originating Agency Identifier (ORI), address, mail code, and level of service (for use when submitting fingerprints using the Live Scan Method).
3. FD 258 Fingerprint Hard Card – for use when submitting fingerprints using the Manual Hard Card Method. BCII 9004, Request for Exemption from Mandatory Electronic Fingerprint Submission Requirement must accompany a FD 258 Fingerprint Hard Card. NOTE: Where Live Scan locations are available, hard card submission will not be accepted.
4. BCII 9004, Request for Exemption from Mandatory Electronic Fingerprint Submission Requirement must accompany a FD 258 Fingerprint Hard Card. NOTE: Where Live Scan locations are available, hard card submission will not be accepted.
5. Computer Security Auditor Approval Handbook describing the following information:

    - Definitions – Refer to Section 13 Appendices – Baseline Requirements and Technology Standards, Pages 3-14
    - Requirements of a Computer Security Auditor
    - Computer Security Auditor Criteria
    - Escrow Requirements
    - Security Audit Requirements
    - Terms and Conditions
    - Geographical Locations
    - Social Security Number Privacy Statement
    - Fee Schedule - PENDING
    - Disqualifying Offenses
    - AB 578 - Chapter 621
    - AB 1738 - Chapter 520
    - Program Regulations - PENDING
    - Baseline Requirements and Technology Standards
    - Forms

SECTION 4
REQUIREMENTS OF A
COMPUTER SECURITY AUDITOR

Individuals proceeding with the ERDS Computer Security Auditor Approval process must comply with the following:

1. Submit a completed ERDS 0002, Application for Computer Security Auditor Approval to the address on the application. This application must be dated and signed under penalty of perjury attesting to the fact that the applicant has read the materials contained in the Computer Security Auditor Approval Package. A signed application will indicate that the applicant understands and agrees to the established Terms and Conditions.
2. Individuals must complete Section 1 of ERDS 0002, Application for Computer Security Auditor Approval, indicating Geographical Location they are interested in auditing, i.e., Northern, Central, Southern California or Statewide.
3. Submit a check or money order, no cash, for all fees. Fees are non-refundable (refer to Fee Schedule).
4. Submit additional Computer Security Auditor criteria as outlined in Section 5 of this handbook
5. Submit a signed Social Security Number Privacy Statement
6. Submission of fingerprints by one of the following methods:

NOTE: ***Beginning July 1, 2005 all applicant fingerprint submissions must be transmitted electronically (Follow Step a). In some rare circumstances, fingerprint Hard Cards will be accepted if an applicant provides the Department of Justice with a valid reason for not submitting by Live Scan and the Department of Justice waives the requirement of electronic submission. In those instances, the Request for Exemption From Mandatory Electronic Fingerprint Submission Requirement form BCII 9004 must be submitted (Follow Step b).***

a. Submitting Fingerprints via BCII 8016, Request for Live Scan (Electronic Submission) Service may be obtained at most law enforcement agencies. To obtain the most current locations where live scan fingerprint services are available, an applicant may go on-line to the Attorney General's home page or the Applicant Fingerprint Submission page, both found at http://caag.state.ca.us.

The BCII 8016 Request for Live Scan Service must be submitted to the law enforcement and/or other agency providing the live scan services. Applicants are encouraged to access the fingerprint web site, www.caag.state.ca.us/fingerprints for fingerprinting locations in their area and to determine if an appointment for fingerprinting is required, if additional fees may be charged for the fingerprint rolling services, and

the acceptable method of payment. Fingerprinting fees totaling $57.00 ($32.00 for the state fingerprint submissions and $24.00 for the federal fingerprint submission) will be required. Amounts do not include separate fees that may be charged by an agency for rolling fingerprints

After the live scan services are performed, the applicant will receive a copy of the BCII 8016, Request for Live Scan Service. Submit ERDs 0002, Application for Computer Security Auditor Approval along with the copy of the BCII 8016, Request for Live Scan Service as proof of fingerprinting.

b. Fingerprints Submitted via FD 258, Fingerprint Hard Card (Manual Submission) maybe submitted, if fingerprinting has been provided by a certified fingerprint roller. The individual needs to submit their FD 258, Fingerprint Hard Card along with the ERDS 0002, Application for Computer Security Auditor Approval. The fingerprint card **must** include the certified fingerprint roller's signature and certification number next to their signature. If the quality of the fingerprint image is poor, if data fields are not properly completed, or the signature and certification number of the fingerprint roller are missing, the applicant fingerprint card will be rejected and returned to the applicant.

   In addition, the FD-258, Fingerprint Hard Card must be accompanied by a BCII 91004, Request for Exemption From Mandatory Electronic Fingerprint Submission Requirement. Fingerprinting fees totaling $57.00 ($32.00 for the state fingerprint submissions and $24.00 for the federal fingerprint submission) are required. A **separate** check or money order made payable to the "California Department of Justice-ERDS Program" must accompany the ERDS 0002, Application for Computer Security Auditor Approval. The ERDS 0002, Application for Computer Security Auditor Approval, fingerprints, and separate set of fees must be mailed to the Department of Justice at the address indicated on the application.

c. Individuals residing outside of California and applying for certification in California who cannot be fingerprinted in California must have their fingerprints rolled at a law enforcement agency in their state of residence. A fingerprint-rolling fee may be collected by the law enforcement agency when fingerprints are taken.

   If living outside California, fingerprints must be submitted via FD 258, Fingerprint Hard Card with the ERDS 0002, Application for Computer Security Auditor Approval. Fingerprint processing fees totaling $57.00 ($32.00 for the state fingerprint submission and $24.00 for the federal fingerprint submission) are required.

SECTION 5
COMPUTER SECURITY AUDITOR CRITERIA

The Computer Security Auditor Approval is based on an individual's significant experience and fingerprint background requirements. Therefore, any individual or company/employer seeking Computer Security Auditor Approval for employee's must submit an ERDS 0002, Application for Computer Security Auditor Approval on an individual basis.

The Approval of a Computer Security Auditor will be based on the following criteria:

1. Receipt of completed ERDS 0002, Application for a Computer Security Auditor Approval, including ERDS 0004, Computer Security Auditor Significant Experience Requirements, Attachment A.
2. Receipt of appropriate fees – Refer to Fee Schedule.
3. Proof of submission of fingerprints (Copy of BCII 8016, Request for Live Scan Service or FD 258, Fingerprint Hard Card) for individuals designated as having secure access, submission of fingerprinting fees and determination of no disqualifying offenses.
4. To qualify for applying for a Computer Security Auditor Approval, the applicant must provide either:

    a. Persons who possess the following certifications, and are in good standing with the certifying organization, may submit the following certifications toward satisfying the criteria for significant experience:
        - Certified Internal Auditor (CIA), The Institute of Internal Auditors.
        - Certified Information Systems Auditor (CISA), Information Systems Audit and Control Association, or

    b. Persons who possess the following certifications, and are in good standing with the certifying organization, may submit the following certifications toward satisfying the criteria for significant experience:
        - Certified Fraud Examiner (CFE), Association of Certified Fraud Examiners (ACFE), who has at least two years of experience in the evaluation and analysis of Internet security design, the conduct of security testing procedures, and specific experience performing Internet penetration studies. This experience must have been within the 5-year period preceding the application date for approval.
        - Certified Information Systems Security Professional (CISSP), International Information Systems Security Certification Consortium (ISC) who has at least two years of experience in the evaluation and analysis of Internet security design, the conduct of security testing procedures, and specific experience performing Internet penetration studies. This experience must have been within the 5-year period preceding the application date for approval.

- Persons who meet the requirements for either of the two certifications defined above in every way except for a formal exam may be approved if they achieved a Global Information Assurance Certification (GIAC), Global Systems and Network Auditor (GSNA) Certification through the Systems and Networks Security (SANS) Institute.

SECTION 6
APPLICATION PROCESSING

The ERDS program will respond to the auditor with an approval or denial within an estimated timeframe of 90 days of receipt of the application and all associated documents.

One of the following steps will be taken following Department of Justice's review of the ERDS 0002, Application for Computer Security Auditor Approval.

A. If the application is determined to be incomplete:

An incomplete application is determined by the following criteria
1. Rejected fingerprints
2. Missing/illegible data
3. Incorrect/missing fees

ERDS Program will:

Return the application to the applicant with a cover letter explaining the reason for return.

Applicant will:

Have thirty (30) days to respond.
If the applicant does not respond within thirty (30) days, the application shall be considered void. Any subsequent application shall require submission of new fees.

Note: Within the thirty (30) days, the estimated Department of Justice response timeframe of ninety (90) days is suspended until the application has been resubmitted and received by the ERDS Program.

B. If the application is determined to successfully meet all criteria:

Approval of application for Computer Security Auditor:

ERDS Program will proceed by:
1. Issuing an Approval Letter
2. Issuing an Computer Security Auditor Approval Certificate
3. Post the Approved Auditor's Information on the Attorney General's Web Site

The certificate will reflect the following:

- Date of Issuance
- Expiration Date
- Auditor Name
- Auditor Approval Number

C. If the application is determined to be denied:

ERDS Program will proceed by:

1. Issuing a letter of denial, informing the applicant of the reason for denial.
   Refer to Section 9 – APPEAL PROCESS

SECTION 7
AUDITOR RENEWAL

The ERDS Approval of a Computer Security Auditor, as issued by the Department of Justice to the auditor, including those designated employees and/or business entities of the auditor, shall remain in effect for a period of three (3) years unless termination has been issued to the individual by the Department of Justice. An ERDS 0002, Application for Computer Security Auditor Approval, indicating Renewal of a Computer Security Auditor Approval, shall be submitted to the Department of Justice at the end of the three (3) year period for auditors wishing to renew their approval certification.

SECTION 8
TERMINATE, SUSPEND OR WITHDRAWAL

Termination / Suspend:

A County Recorder may refuse to enter into a contract with any party or may terminate or suspend access to a system for any good faith reason. Government Code section 27391(c). The County Recorder will make notification to Department of Justice in the case of a termination or suspension. Government Code section 27394 (f).

In addition to a County Recorder's notification of termination or suspension, the Department of Justice shall terminate or suspend an approval based on a subsequent notification of a disqualifying offense and/or any breaches of ERDS security Government Code section 27395 (a) and Government Code section 27396(a).

For the purpose of ERDS processes, the terms "terminate" and "suspend" are considered interchangeable and are used to designate removal of all privileges of access.

Department of Justice shall issue a letter of termination or suspension to the auditor notifying that Department of Justice approval is invalid.

Department of Justice shall issue a letter to the County Recorder notifying him/her of such termination or suspension and instructing that the County Recorder remove all means of access for the terminated or suspended individual using any login credentials or digital certificates provided for access.

Withdrawal from Approved Computer Security Auditor Certification

An Approved Computer Security Auditor choosing to withdraw their Approved Certification shall submit a completed ERDS 0010, Application for Withdrawal, to the Department of Justice.

Department of Justice shall issue a letter of Computer Security Auditor Termination to the Auditor; notifying he/she that the Department of Justice certification has been withdrawn.

Department of Justice shall issue a letter to the County Recorder notifying him/her of such withdrawal and instructing that the County Recorder remove all means of Auditor access.

All Approved Computer Security Auditor Certification fees are non-refundable. If at a later date, the Auditor chooses to have his/her Certification re-instated, the Auditor must re-apply and complete the application process including payment of fees. The Auditor will be issued a new Certification Number.

The Auditor will retain his/her secure access status unless approval has expired or has been terminated or suspended by the County Recorder or the Department of Justice.

SECTION 9
APPEAL PROCESS

The following steps are available based on either denial of an application or termination/suspension of a certificate.

A. Denial of Application

A denial must be appealed in writing within thirty (30) days of the ERDS program notification to the applicant:

- A program committee will review a request for an Appeal.
- A determination shall be made in writing to the appellant:

  Appeal denied – ERDS staff shall issue a letter informing the appellant.

  Appeal granted – ERDS staff shall issue a letter informing the appellant of the decision to grant the appeal.

B. Termination or Suspension of Certification

A termination or suspension of a notification of approval must be appealed in writing within thirty (30) days of the ERDS program notification to the certificate holder:

- A program committee shall review a request for an Appeal.
- A determination shall be made in writing to the appellant:

  Appeal denied – ERDS staff shall issue a letter informing the appellant.

  Appeal granted – ERDS staff shall issue a letter informing the appellant of the decision to grant the appeal.

SECTION 10
REQUEST FOR DUPLICATE CERTIFICATE AND/OR COPIES

ERDS 0006, Request for Replacement of Certificate or Application Documents is to be utilized for requesting the documents listed below.

Duplicate Certificate:

An approved auditor may request a duplicate Certificate of Approval as an ERDS Computer Security Auditor for the following reasons. The appropriate fee must accompany the request. (Refer to Fee Schedule)

1. A certificate has been lost, stolen or destroyed.
2. A certificate has been mutilated and is no longer usable.
3. Non-receipt of the original certificate.
4. Change in name and/or address reflected on original certificate.

Request for Copies:

An auditor may request copies of documents pertaining to his/her application that are designated as public documents. The request must be accompanied by the appropriate fee. (Refer to Fee Schedule)

1. Application for Computer Security Auditor Approval
2. All documents on file

SECTION 11
ESCROW REQUIREMENTS

A Vendor of a County Recorder's ERDS is required to place the ERDS source code and other materials in an approved Escrow Facility. This section establishes the escrow requirements to be met.

Approved Escrow Facility

An Escrow Company approved pursuant to California Code of Regulations, Title 2, beginning with Section 20630.

Escrow Requirements

Electronic recording delivery system software program source code(s) (or hereinafter: "source code") shall be placed in escrow in order to:
(a) Create a record of all versions, including changes or modifications of the source code materials placed in escrow;
(b) Create a record of all applications for access to the source code materials placed in escrow;
(c) Unless otherwise superseded by a contract between a vendor and a county recorder, preserve the necessary source code information to permit the county recorder to continue the use and maintenance of the source code in the event the vendor is unable, or otherwise fails, to provide maintenance.

Electronic Recording Delivery System Program Source Code(s)

"Electronic recording delivery system software program source code(s)" or "source code" consists of the computer program or programs used for the delivery for recording, and return to the party requesting recording, of a digitized electronic record that is an instrument affecting a right, title, or interest in real property or a digital electronic record that is an instrument of reconveyance, substitution of trustee, or assignment of deed of trust and store that digitized or digital electronic record to a storage media for later retrieval and reporting

Vendor Letter of Deposit

Within a timeframe established by the County Recorder of any submission of source code materials by a vendor to an approved escrow facility, the vendor shall acknowledge in writing to the affected County Recorder that they have placed their source code or codes in escrow. The vendor letter of deposit shall include a description of submitted materials sufficient to distinguish them from all other submissions.

The vendor letter of deposit shall state:

(1) That all source code information and materials required by these regulations and other applicable law are included in the deposit.
(2) The name of the approved escrow company and the location of the escrow facility where the source code materials have been placed in escrow. The escrow company, its officers, and directors, shall not hold or exercise any direct or indirect financial interest(s) in the vendor.
(3) The escrow company, its officers, and directors, shall not hold or exercise any direct or indirect financial interest(s) in the vendor.
(4) That the escrow company meets the "requirements for escrow facility" as stated in the Escrow Requirements.

Requirements for Submission

(a) The vendor shall submit the source code, as defined in (c) below, to an approved escrow company for placement in the escrow facility.
(b) For each source code, the materials placed in escrow must be sufficient to maintain every related electronic software program used or intended to be used by any county recorder.
(c) The content of escrow materials should be compiled to allow complete and successful restoration of the ERDS in its production environment with confirmation by a production verification test by qualified personnel using only this content. It should include, but not limited, to the following items:

(1) All software modules-components purchased by the Vendor, and used in building the ERDS.
(2) All licenses and security license keys necessary for successful installation and use of these components.
(3) Full documentation (functional descriptions, interface specifications, instructions for installations and use) for all purchased components from their original manufacturers.
(4) Technical support and warranty information from original manufacturers of the components.
(5) Architectural documentation showing usage of these components in the built ERDS.
(6) All software modules-components (in original source code version) developed by the Vendor and used in building the ERDS.
(7) Full engineering design documentation (diagrams, dictionaries, specifications, unit test scripts) for each developed component.
(8) System architectural design documentation.
(9) Bill of Materials – detailed list of all system components purchased and developed.
(10) Detailed deployment diagrams for production environment and deployment specifications with all "build" and "make" instructions.
(11) Detailed Deployment Plan specifications.

(12) Installation and deployment scripts, configuration files, data definition language scripts, and other instructions necessary for full install of the ERDS.
(13) Data loads used for initiation of production with loading scripts or harnesses.
(14) Production Verification Test (content and expected results).
(15) Copy of all compilers and other deployment tools, if purchased separately from OS software, used with their versions mentioned.
(16) Copy of Operating System "sysgen" instructions used for platform preparations for ERDS deployment at different nodes.
(17) Copy of all OS patches used for platform preparations for ERDS deployment at different nodes.

Updates to Submission

Once used to record a digital or digitized record in any electronic recording delivery system, no source code materials in escrow may be changed or modified. Substantive Modifications as described below requires that a new escrow be established.

Substantive Modifications

The following defines substantive modifications:

(1) To source code –
- Modifications or changes leading to a different functional behavior of ERDS or its part (application)
- Modifications of call signatures in interfaces with purchased components
- Modifications of data structures or structural database objects (add table or add column to a table)
- Any change that require modification of deployment procedures.

(2) To Compilers –
- New version of a compiler is as a substantive modification, if the existing ERDS source code cannot be compiled error free (including warnings) without changes of the source code.

(3) To related software (i.e., libraries or purchased components) –
- Any change in a component or module functionality
- Any change in call signatures of modules or call interfaces

(4) To an operating system –
- Any change or upgrade that relates to security settings or security policies
- Cumulative update to a new service pack level

(5) To a System and/or network devices
- Any changes to the server, workstation and/or network devise hardware/software configuration that impacts the ERDS system.
- Any changes to the network architecture/network design as it pertains to the ERDS.

Elaboration: If an ERDS is designed to be independent of the operating system, only ERDS source code needs to be tested, archived and escrowed. For ERDS application source code, any modification is substantive and must be tested, archived and escrowed.

If an ERDS cannot be designed to be independent of the operating system, then for any operating system, compiler or related software (i.e. libraries), any patch or "hotfix" that corrects one or more vulnerabilities, at least one of which presents "high risk" of system compromise, must be considered "substantive". Such a patch or hotfix must be archived and escrowed to ensure subsequent installations using the original operating system are properly patched.

Deposit Software Modifications into Escrow

(a) Prior to being used to record digital or digitized documents in any electronic recording delivery system, the vendor shall submit all source code changes or modifications into escrow in the same manner and under the same conditions in which the source code materials originally were placed in escrow.

(b) Within a timeframe established by the County Recorder of any submission of changed or modified source code, the vendor shall notify each affected County Recorder that the source code placed in escrow has been changed or modified.

Separation of Interest of Escrow Company with Vendor

A vendor may enter into a written agreement with any escrow company for deposit of each source code. However, the escrow company, its officers, and directors, shall not hold or exercise any direct or indirect financial interest(s) in the vendor.

Requirements for Escrow Facilities

For all electronic recording delivery system software program source code materials each escrow facility shall:
(a) Provide a secure and safe environment in which the humidity, temperature, and air filtration are controlled on a 24-hours-a-day, 7-days-a-week basis. The humidity shall be maintained at 35 percent, plus or minus 2 percent, and the temperature shall be maintained at 65 degrees, plus or minus 3 degrees, Fahrenheit.
(b) Maintain storage away from electrical, magnetic, and other fields which could potentially damage computer media over time.
(c) Have backup capability to maintain the properly secured environment in the event of power outages or natural disasters.
(d) Maintain physical security of the escrow facility with controlled and restricted access to all materials placed in escrow.

(e) Store each source code separately. The source code materials placed in escrow shall be secured in a single container and no other material shall be placed in that container.

Conditions for Access to Materials Placed in Escrow.

No access to materials placed in escrow shall occur except as specified in this section.
(a) County Recorder shall provide and maintain a list of people having access to escrow materials. Escrow facility will keep a log of access to the materials stored.
(b) Upon a finding by the Attorney General, county recorder, or district attorney that an escrow facility or escrow company is unable or unwilling to maintain materials in escrow in compliance with these regulations.
(c) The Attorney General may, in furtherance of these regulations, for cause at any time, audit source code materials placed in escrow with an escrow facility for purposes of verifying the contents.
(d) An approved computer security auditor shall have access to any aspect of an electronic recording delivery system, in any form requested to complete their certification of the system. Computer security auditor access shall include, but not be limited to, permission for a thorough examination of source code and the associated approved escrow facility, and necessary authorization and assistance for a penetration study of that system.
(e) The vendor shall be entitled at reasonable times during normal business hours and upon reasonable notice to the escrow company during the term of the escrow agreement to inspect the records of the escrow company pertaining to the escrow agreement.

Integrity of Materials Placed in Escrow

No person having access to the electronic recording delivery system software program source code materials shall interfere with or prevent the escrow representative from monitoring the security and the integrity of the electronic delivery system software program source code materials.

Minimum Terms Required in Agreement

The terms of the agreement between the vendor and the escrow company shall include, but not be limited to, the following elements:

(1) The escrow company, its officers, and directors, do not hold or exercise any direct or indirect financial interest(s) in the vendor.

(2) The vendor, its officer, and directors, do not hold or exercise any direct or indirect financial interest(s) in this escrow company.

(3) No source code placed in escrow shall be changed or modified except as permitted in this chapter.

(4) The time period for the escrow agreement and the date for renewal of the agreement.

(6) A provision that the escrow agreement may be renewed for additional periods.

(6) The due date for renewal shall be no later than 30 days before expiration of the escrow agreement. In the event that the contract is not renewed, the escrow company shall so notify the County Recorder and the Attorney General.

(7) In the event that a vendor does not enter into an escrow arrangement with the escrow company to renew the escrow contract, a County Recorder may negotiate directly with an escrow company for continuance of the escrow, and shall so notify the Attorney General and the vendor in writing within 30 days of the new contract.

(8) In the event that the escrow company is notified by a county recorder of the occurrence of a condition as defined in the escrow agreement allowing access to electronic recording delivery system software program source code materials, the escrow company shall immediately so notify the vendor and the Attorney General and shall provide a copy of the notice from the county recorder.

(9) If the vendor provides an objection in writing within 10 days of the mailing or other service of the notice to the vendor, the escrow company shall not allow access. If the vendor does not object as provided in this subdivision, the escrow company shall permit access to the deposit to the county recorder. For the purposes of this section "object" or "objection" means the delivery by certified mail of an affidavit or declaration to the escrow company by the vendor, with a copy to the county recorder which is demanding access and a copy to the Attorney General. The objection shall state that an access condition either has not occurred or no longer exists. Upon receipt of the objection, the escrow company shall not permit access and shall continue to store the deposit pursuant to the escrow agreement.

(10) A requirement that the Escrow Company submit a copy of every electronic recording delivery system escrow agreement to the County Recorder. The copy shall be submitted by the escrow company within ten days of the date the escrow agreement is signed.

(11) For every submission of an electronic recording delivery system escrow agreement, maintain records which sufficiently identify and describe the materials deposited in escrow to determine compliance with the agreement between the vendor and the escrow company. The escrow company shall not be required to verify the content of the materials submitted.

(12) Notify, in writing, the County Recorder within five days of the initial deposit of electronic recording delivery system source code. The notice shall include the name of the vendor and a list describing each of the items comprising the initial submission.

(13) Notify, in writing, the County Recorder within five days of the termination of any electronic recording delivery system escrow agreement.
(14) Notify, in writing, the Attorney General within five days of the change of the name of the company or the name of the escrow facility, together with the address, phone number, and name of the contact person for the company and/or facility.

Retention of Electronic Recording Delivery System Materials

Records maintained by the escrow company pursuant to these regulations and other applicable law shall be retained for the term of the escrow agreement, and for an additional period of 22 months.

The escrow agreement shall provide for the disposition of the materials placed in escrow.

State Not Liable for Any Costs or Any Other's Actions

Neither the Attorney General nor the State of California shall be responsible for any of the fees claimed by the vendor, election jurisdictions, or the escrow company to establish the escrow contract. Further, neither the Attorney General nor the State of California is a party to the agreement and shall not incur any liability for the actions of the parties involved in this escrow agreement.

SECTION 12
SECURITY AUDIT REQUIREMENTS

Nature and Frequency of Electronic Recording Delivery System Computer Security Audits

An initial audit is required before any Electronic Recording Delivery System may be implemented. (See Gov. Code 27394(a).) An approved Computer Security Auditor shall conduct a security audit of a County Recorders Electronic Recording Delivery System and it's Authorized Submitter(s) for the purpose of validating that the system is reasonably secure from vulnerabilities and unauthorized penetration. (See Gov. Code 27394(c).)

Thereafter, an approved ERDS Computer Security Auditor shall audit the Electronic Recording Delivery System annually for the system to remain certified and whenever a substantive modification is made to the Electronic Recording Delivery System.

A computer security audit is a systematic, measurable, technical assessment of how the baseline security requirements required by the Attorney General are applied to an Electronic Recording Delivery System.

Security Audit for Initial Implementation and Substantive Modification

The approved Computer Security Auditor shall conduct an end-to-end security audit of the Electronic Recording Delivery System in accordance with generally accepted information security practices. The approved Computer Security Auditor must document his/her findings during the audit. Information in an audit report shall include, but is not necessarily limited to, the following:

1. Demonstration of the proposed system in its intended operational environment in a test mode. Testing shall include the following:

    - A review of the network configuration showing all network nodes;
    - An inventory of hardware, software and network components comprising the proposed system;
    - An inventory of users and roles assigned to operate the system;
    - Tests showing that digital and digitized documents are neither transmitted nor stored in an unencrypted format anywhere in the system.
    - Tests showing that transmissions only occur between authorized parties. The operational environment must be mapped to identify (a) the servers, workstations and network nodes visible from any ERDS workstation or server, (b) the ERDS workstations and servers visible from any non-ERDS workstation or server, and (c) the users and roles authorized to access ERDS workstations and servers.

- Remnants of sessions, transmissions and documents are not stored once the user initiating the session and transmitting documents has logged out or been disconnected (either physically or logically).
- A review of the system design showing all components;
- A review of the source code or selected (or all) software components;
- The test environment must simulate authorized and unauthorized users operating in the roles of county recorder, authorized submitter, agent of authorized submitter, and Internet user.

2. A Description of Deposit Materials showing that the source code has been deposited in Escrow with an Escrow Company approved pursuant to Chapter 6, Division 7, Title 2 of the California Administrative Code, beginning with Section 20630.

Annual Audit

The County Recorder shall obtain an audit of the Electronic Recording Delivery System at least once every year. An authorized Computer Security Auditor must perform the audit. The audit will be conducted in the system's operational environment. Testing shall include the following:

1. A review of the network configuration showing all network nodes;
2. An inventory of hardware, software and network components comprising the proposed system;
3. An inventory of users and roles assigned to operate the system;
4. Tests showing that digital and digitized documents are neither transmitted nor stored in an unencrypted format anywhere in the system.
5. Tests showing that transmissions only occur between authorized parties. The operational environment must be mapped to identify (a) the servers, workstations and network nodes visible from any ERDS workstation or server, (b) the ERDS workstations and servers visible from any non-ERDS workstation or server, and (c) the users and roles authorized to access ERDS workstations and servers.
6. Remnants of sessions, transmissions and documents are not stored once the user initiating the session and transmitting documents has logged out or been disconnected (either physically or logically).
7. Collected audit data correlates to actual activity and all auditable events are collected for audit.
8. Description of Deposit Materials showing that the source code has been deposited in Escrow with an approved Escrow Company.

Audit Report Format

The format for both the Initial and Annual Security Audit shall include, but is not necessarily limited to, the following:

1. A non-technical, business-oriented executive overview.

2. A detailed technical observation/recommendation section.

3. A summary of recommendations in a task-list format.

4. A ranking of the vulnerabilities/weaknesses found during the audit will be documented utilizing a High, Medium, and Low level-of-risk categorization. Show a correlation of each security vulnerability/weakness to a business risk.

    - High-level vulnerabilities/weaknesses will be classified as vulnerabilities/weaknesses found to pose a hazardous level of risk to the confidentiality, integrity and/or availability of the data and services provided by the ERDS.
    - Medium-level vulnerabilities/weaknesses will be classified as vulnerabilities/weaknesses that pose a significant level of risk to the confidentiality, integrity and/or availability of the data and services provided by the ERDS.
    - Low-level vulnerabilities/weaknesses will be classified as vulnerabilities/weaknesses that do not pose a significant level of risk to the confidentiality, integrity and/or availability of the data and services provided by the ERDS.

5. A diagram depicting results where applicable.

6. A description of the approved Computer Security Auditors methodology.

7. A recommendation for any additional precautions needed to ensure that the system is secure.

The initial security audit report shall be further subdivided and include but will not be limited to the following categories of items:

Audit Categories	System Passes/Fails	Comments, Notes
Safety and security of the system:		
No evidence of breaches during testing		
System performed to specifications		
Physical security measures are adequate to prevent unauthorized access		
User survey conducted with satisfactory results in security confidence		
Vulnerability of the electronic recording delivery system to fraud or penetration:		
All documents entering and exiting the system were encrypted per ERDS requirements		
Mechanisms for encrypting met the ERDS		

Baseline Requirements and Technology Standards		
Access control measures acted to restrict access based on identity and organizational role		
Authentication correctly identified authorized users		
Satisfactory testing conducted submitting sample documents from location X		
Results of testing of the system's protections against fraud or intrusion, including security testing and penetration studies:		
Penetration testing concluded that the system was not exploitable based on the tests conducted		
Security events were properly recorded and detected in audit logs		
Recommendations for any additional precautions needed to ensure that the system is secure:		
Auditor recommends timing of audits increase/decrease		
Encryption keys should be increased by X		
The organization needs to add to or improve security policies		
Recommendation to add more constrictive controls		
Recommendation to authorize continued use		

System Authorization Decision

Audit findings shall be conveyed to the County Recorder in a written audit report. The initial audit report shall be attached to the ERDS 0001, Application for System Certification, submitted by the County Recorder when applying with Department of Justice for system certification. Thereafter, an annual audit report will be forwarded by the County Recorder to the Department of Justice consistent with the Terms and Conditions-System Certification. There are two types of decisions that can be rendered by the Department of Justice:

1. Authorization to operate; and

2. Denial of authorization to operate.

Authorization to Operate

If, after assessing the results of the Computer Security Audit, the Department of Justice deems that the Electronic Recording Delivery System has met the Baseline Requirements and Technology Standards established for an Electronic Recording Delivery System with no high-level or medium-level vulnerabilities/weaknesses, an authorization to operate will be issued for the Electronic Recording Delivery System. The authorization will indicate that the Electronic Recording Delivery System is authorized to operate without any significant restrictions or limitations on its operation.

Although not affecting the authorization to operate decision, the County Recorder should take specific actions to reduce or eliminate any low-level vulnerabilities/weaknesses identified by the Computer Security Auditor where it is cost-effective to do so. The County Recorder shall, as the system owner, establish a disciplined and structured process to monitor the effectiveness of the security controls for the Electronic Recording Delivery System.

Denial of Authorization to Operate

If, after assessing the results of the Computer Security Audit, the Attorney General's authorizing official deems that the risk to agency operations, agency assets, or individuals is unacceptable, the authorization to operate the Electronic Recording Delivery System will be denied. The system will not be certified and will not be placed into operation. If the system is currently in operation, all activity shall be halted.

To address the security related deficiencies the County Recorder shall submit a plan of action and milestones to be used by the Department of Justice and Computer Security Auditor to monitor the progress in correcting deficiencies noted during the security audit.

When the security related deficiencies have been addressed and confirmed by the Computer Security Auditor, the County Recorder may request the Department of Justice for reconsideration for authorization to operate and system certification.

The County Recorder shall, as the system owner, establish a disciplined and structured process to monitor the effectiveness of the security controls for the Electronic Recording Delivery System.

Filing Procedures

Upon completion, the final Computer Security Auditors "Security Audit Report", the Attorney General's "System Certification Decision" recommendation and any response to any recommendations shall be transmitted to the board of supervisors, the county recorder, the county district attorney, and the Attorney General. These reports shall be exempt from disclosure under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1).

SECTION 13
APPENDICES/FORMS

The Appendices include the following documents:

Terms and Conditions – Auditor
Geographical Locations
Social Security Number Privacy Statement
Fee Schedule - PENDING
Disqualifying Offenses
Statutory Authority, Chapter 621
Statutory Authority, Chapter 520
Regulations – PENDING
Baseline Requirements and Technology Standards

TERMS AND CONDITIONS – COMPUTER SECURITY AUDITOR

Electronic Recording Delivery System Computer Security Auditor must review and agree to the Terms and Conditions Statement to obtain an Approval by the Department of Justice Electronic Recording Delivery System Program. The Terms and Conditions include the requirement to protect the confidentiality, integrity, and availability of the electronic recording delivery system.

1. Scope
   - The Terms and Conditions apply to all personnel, equipment, software, systems, networks, communication links, and facilities supporting and/or acting on behalf of the Approved Computer Security Auditor.
   - These Terms and Conditions do not confer, grant, or authorize any rights or privileges to any entity or person other than the Approved Computer Security Auditor and/or those acting on the behalf of the Approved Computer Security Auditor.

2. Personnel Security

   - The Approved Computer Security Auditor shall be responsible for the actions of any person or entity acting on their behalf and/or providing services in support of the Approved Computer Security Auditor.
   - All employees and/or business entities acting on behalf of the computer security auditor shall be subject to the fingerprint background requirements prior to a auditor's approval.
     The Approved Computer Security Auditor shall maintain a current list of all personnel and/or business entities employed by and/or acting on their behalf that have been granted secure and/or authorized access to any electronic recording delivery system.

3. Site Security

   - The site housing all hardware and software associated with the capture, development and/or transmission of electronic recording delivery system security testing and audit reports shall be adequately secured at all times to reasonably protect against theft, damage, and/or unauthorized access or use by any person.

4. Information Security

   - The data residing in the electronic recording delivery system is confidential and the use of this information for any purpose other than the purpose for which it was expressly provided is strictly prohibited.
     Violation of the electronic recording delivery system security may subject the Approved Computer Security Auditor and/or those acting on the behalf of the Approved Computer Security Auditor to criminal and/or civil

liability, and may result in termination of the Approved Computer Security Auditor's certification.

Every person as designated by a County Recorder who, in the course of their normal duties collects, processes, and/or facilitates the capture, development and/or transmission of electronic recording delivery system data shall be required to sign an ERDS 0011, Secure and Authorized Access Statement, acknowledging that they understand their responsibilities for protecting confidential electronic recording delivery system information, the restrictions concerning the use of such information, and the penalties for misuse. Signed copies of the Certification form shall be retained by the County Recorder and shall be made available to the Attorney General upon request.

- Computer Security Auditor agrees to maintain policies and procedures in accordance with NIST SP 800-53. To review NIST SP 800-53 go to: http://csrc.nist.gov/publications/nistpubs/index.html

5. Security Violations

- All security violations or suspected security violations shall be immediately reported to the Attorney General. Reports of security violations shall include the date of the incident(s), the parties involved (if known), the nature and scope of the incident, and any action(s) taken, including steps to protect against future violations.
- The Attorney General reserves the right to investigate all reported or suspected security violations and to take any action deemed appropriate and/or necessary to protect the security and stability of the electronic recording delivery system, including termination of the Approved Computer Security Auditor certification.

6. Quality Control

- All equipment associated with the capture and transmission of electronic recording delivery systems information shall be adequately secured at all times by assuring that software upgrades (including the installation of any patches deemed necessary by the manufacturer) shall be applied in a timely fashion and shall remain current.

GEOGRAPHICAL LOCATION(S)

THESE COUNTIES ARE USED TO SELECT GEOGRAPHICAL LOCATION (S) INTERESTED IN AUDITING:

Northern California:

Amador, Alpine, Butte, Colusa, Del Norte, El Dorado, Glenn, Humboldt, Lake, Lassen, Marin, Mendocino, Modoc, Napa, Nevada, Placer, Plumas, Sacramento, Shasta, Sierra, Siskiyou, Solano, Sonoma, Sutter, Tehama, Trinity, Yolo, Yuba.

Central California:

Alameda, Calaveras, Contra Costa, Fresno, Inyo, Kern, Kings, Madera, Mariposa, Merced, Mono, Monterey, San Benito, San Francisco, San Joaquin, San Luis Obispo, San Mateo, Santa Clara, Santa Cruz, Stanislaus, Tulare, Tuolumne.

Southern California:

Imperial, Los Angeles, Orange, Riverside, San Bernardino, Santa Barbara, San Diego, Ventura.

STATE OF CALIFORNIA
DEPARTMENT OF JUSTICE
Division of California Justice Information Services
CJIS Operation Support Bureau
Electronic Recording Delivery System Program

SOCIAL SECURITY NUMBER
PRIVACY STATEMENT

USE OF SOCIAL SECURITY NUMBER: You are required by law to provide your Social Security Number (SSN) or your application will not be processed for ERDS Certification.

The SSN is required and will be used by the Department of Justice for identification and verification purposes. The SSN provided on the application will not be made available for public inspection. The SSN is a standard data element included in the Department of Justice criminal offender record information systems as defined in Penal Code section 13125. In addition, Family Code section 17520 requires that any state Department issuing certificates to engage in an occupation shall collect the SSN of the applicant.

Collection of your SSN is mandatory. Failure to provide the information will result in the rejection of your application for certification.

I have read the Privacy Statement and understand the Privacy Statement information.

Signature: _____ Date _____

Print name: _____

Applicant should keep a copy of this for their records

FEE SCHEDULE

Process	Fee	Trans Code ASD to assign	Trans Title (for DOJ use only)	Fund
Vendor				
Initial Vendor and Software Certification	TBD			Electronic Recording Authorization Account
Renewal Certification	TBD			Electronic Recording Authorization Account
County				
System Administration Fee	This fee is allocated to each participating county by the total documents recorded and filed as reported to the Office of the Insurance Commissioner, as provided in Government Code section 27296, for the previous year. The formula to determine a county's proportionate cost is set by the total documents recorded and filed per individual participating counties divided by the total documents recorded and filed by all participating counties. The percentage figure obtained for each participating county is applied to the estimated annual costs of the Attorney General to arrive at an individual participating county figure.			Electronic Recording Authorization Account
MISC				
Fingerprint (State) Hard Card & Live Scan	$32.00			Fingerprinting Fee Account
Fingerprint (Fed) Hard Card & Live Scan	$24.00			Fingerprinting Fee Account
Returned Item (DOJ Manual 13230)	$10.00			Electronic Recording Authorization Account
Re-issuance of Certification (lost/destroyed)	$10.00			Electronic Recording Authorization Account
Copies (Admin Bulletin 05-08)	.30 per page			Electronic Recording Authorization Account

ELECTRONIC RECORDING DELIVERY SYSTEM
SECURE ACCESS
DISQUALIFYING OFFENSES

For the purposes of fingerprinting, Secure Access[1] refers to an individual's ability to submit documents for recording in a digitized environment. No person shall be granted secure access to an electronic recording delivery system if he or she has been convicted of a felony, has been convicted of a misdemeanor related to theft, fraud, or a crime of moral turpitude, or if he or she has pending criminal charges for any of these crimes. A plea of guilty or no contest, a verdict resulting in conviction, or the forfeiture of bail, shall be a conviction within the meaning of GC section, 27395 (a), irrespective of a subsequent order under Section 1203.4 of the Penal Code.

A felony conviction or pending charges involving the following offenses will be justification for denial of secure access:

Felony:

• Homicide	• Forgery
• Robbery	• Arson
• Assault	• Drugs
• Kidnapping	• Sex
• Burglary	• Driving under the Influence
• Theft	• Hit and Run
• Motor Vehicle Theft	• Weapons
• Escape	• Bookmaking
• Identity Theft	• Unauthorized Access to Computers

And/Or

Any other state or federal felony convictions including pending charges, involving dishonesty, fraud or deceit, which are substantially related to the qualifications, functions, or duties of a person engaged in the secure access of an electronic recording delivery system as described within Government Code Sections 27390-27399.

A misdemeanor conviction or pending charges involving the following offenses will be justification for denial of secure access:

Misdemeanor:

• Misdemeanor manslaughter	• Liquor Laws
• Assault and Battery	• Disturbing the Peace
• Theft	• Malicious Mischief
• Drugs	• Driving under the Influence
• Sex	• Gambling
• Checks and Access Cards	• Trespassing
• Vandalism	• Contributing to the delinquency of a minor
• Identity Theft	• Unauthorized Access to Computers

And/Or

Any other state or federal felony convictions, including pending charges, involving "moral turpitude" [People v. Castro (1985) 38 Cal. 3d 301], provided that the crimes are substantially related to qualifications, functions, or duties of a person engaged in the secure access of an electronic recording delivery system as described within Government Code Sections 27390-27399. Examples of crimes involving moral turpitude include murder, rape, assault with a deadly weapon, hit-and-run, arson, robbery, burglary, possession of drugs for sale, sale of drugs, pimping and pandering, etc.

---

[1] The fingerprint requirement does not apply to an individual who has been granted 'authorized access' and who is limited to submitting digital documents only; however, all individuals granted 'Secure Access' or 'Authorized Access' by a County Recorder must sign ERDS 0005, Application Attachment Vendor Employee(s) and/or Business Entity(ies) – Attachment A.

INSERT HERE
AB 578 and AB 1738 HERE

INSERT REGULATIONS HERE

BASELINE REQUIREMENTS AND TECHNOLOGY STANDARDS TO BE INSTERTED HERE

Forms ERDS Requirements Document

This identifies who has responsibility for the completion of and/or submission of the following forms:

Form Name	Vendor	Computer Security Auditor	County Recorder
ERDS 0001 - Application for System Certification			X
ERDS 0002 - Application for Computer Security Auditor Approval		X	
ERDS 0003 - Application for Vendor of Software Certification	X		
ERDS 0004 - Approval of Computer Security Auditor Employee(s) Attachment A		X	
ERDS 0005 - Application Attachment Vendor Employee(s) and/or Business Entity(ies) Attachment A	X		
ERDS 0006 - Request for Replacement of Certificate or Application Documents	X	X	X
ERDS 0008 - Change of Secure and/or Authorized Access			X
ERDS 0009 - Vendor Application Form for Reference(s) Attachment B	X		
ERDS 0010 - Application for Withdrawal	X	X	X
ERDS 0011 - Secure and Authorized Access Statement			X
BCII 8016 - Request for Live Scan Service	X	X	X
FD-258 - Fingerprint Hard Card	X	X	X